

# BUBBLES OF CONGRUENT PRIMES

FRANK THORNE

**ABSTRACT.** In [15], Shiu proved that if  $a$  and  $q$  are arbitrary coprime integers, then there exist arbitrarily long strings of consecutive primes which are all congruent to  $a$  modulo  $q$ . We generalize Shiu's theorem to imaginary quadratic fields, where we prove the existence of “bubbles” containing arbitrarily many primes which are all, up to units, congruent to  $a$  modulo  $q$ .

## 1. INTRODUCTION AND STATEMENT OF RESULTS

In 1997, Shiu [15] proved that if  $a, q$ , and  $k$  are arbitrary integers with  $(a, q) = 1$ , there exists a string of  $k$  consecutive primes

$$p_{n+1} \equiv p_{n+2} \equiv \cdots \equiv p_{n+k} \equiv a \pmod{q}.$$

(Here  $p_n$  denotes the  $n$ th prime.) Furthermore, if  $k$  is sufficiently large in terms of  $q$ , these primes can be chosen to satisfy the bound<sup>1</sup>

$$(1.1) \quad \frac{1}{\phi(q)} \left( \frac{\log \log p_{n+1} \log \log \log \log p_{n+1}}{(\log \log \log p_{n+1})^2} \right)^{1/\phi(q)} \ll k,$$

uniformly in  $q$ .

In this paper we prove an analogous statement for imaginary quadratic fields. If  $K$  is such a field, then the ring of integers  $\mathcal{O}_K$  forms a lattice in  $\mathbb{C}$ , and the primes of  $\mathcal{O}_K$  can be naturally visualized as lattice points. In this setting one may ask whether there are clumps of primes, all of which lie in a fixed arithmetic progression. We prove that this is indeed the case, up to multiplication by units:

**Theorem 1.1.** *Suppose  $K$  is an imaginary quadratic field,  $k$  is a positive integer, and  $a$  and  $q$  are elements of  $\mathcal{O}_K$  with  $q \neq 2$  and  $(a, q) = 1$ . Then there exists a “bubble”*

$$(1.2) \quad B(r, x_0) := \{x \in \mathbb{C} : |x - x_0| < r\}$$

*with at least  $k$  primes, such that all the primes in this bubble are congruent to  $ua$  modulo  $q$  for units  $u \in \mathcal{O}_K$ . Furthermore, for  $k$  sufficiently large (in terms of  $q$  and  $K$ ),  $x_0$  can be*

---

2000 *Mathematics Subject Classification.* 11N13, 11R44.

<sup>1</sup> In Shiu's statement of his results, the initial  $1/\phi(q)$  in (1.1) and the requirement that  $k$  be large are omitted, and the implied constant in (1.1) is allowed to depend on  $q$ . A careful reading of his proof shows that the dependence on  $q$  may be controlled as stated.

chosen to satisfy

$$(1.3) \quad \frac{1}{\phi_K(q)} \left( \frac{\log \log |x_0| \log \log \log \log |x_0|}{(\log \log \log |x_0|)^2} \right)^{\omega_K/h_K \phi_K(q)} \ll k.$$

The implied constant is absolute.

Here  $\omega_K$  denotes the number of units in  $\mathcal{O}_K$ ,  $h_K$  is the class number of  $K$ , and  $\phi_K(q) := |(\mathcal{O}_K/(q))^\times|$ .

*Remarks.* The unit  $u$  will not necessarily be the same for each prime in the bubble (1.2). It would be desirable to obtain a version of Theorem 1.1 where each prime is congruent to  $a$  modulo  $q$ , without the ambiguity involving units. Unfortunately, this ambiguity appears to be unavoidable given our methods of proof.

The restriction that  $q \neq 2$  is not severe; to obtain prime bubbles modulo 2 we may take (for example)  $q = 4$ . For the reason behind this restriction, see Lemma 2.2.

*Example.* Let  $K = \mathbb{Q}(i)$ ,  $q = 5 + i$ , and  $a = 1$ . A computer search reveals that the ball of radius  $\sqrt{7.5}$  centered at  $2 + 17i$  contains three primes, all of which are congruent to  $\pm 1$  or  $\pm i$  modulo  $q$ . Similarly the ball of radius  $\sqrt{23.5}$  centered at  $59 + 779i$  contains six primes, all of which are congruent to  $\pm 1$  or  $\pm i$ . Theorem 1.1 establishes the existence of infinitely many such balls, with  $\omega_K/\phi_K(q) = 1/3$ .

The proof of Theorem 1.1 is an adaptation of Shiu's original proof [15], which we now summarize.<sup>2</sup> Given  $a$  and  $q$  with  $(a, q) = 1$ , Shiu constructs a modulus  $Q(y)$  such that most integers in an interval  $[1, yz]$  which are coprime to  $Q(y)$  are congruent to  $a$  modulo  $q$ . He then constructs a ‘‘Maier matrix’’, the rows of which are short intervals, and the columns of which are arithmetic progressions modulo  $Q(y)$ . By an appropriate version of the prime number theorem for arithmetic progressions (2.1), most primes in the matrix are congruent to  $a \pmod{q}$ . A counting argument establishes the existence of strings of congruent primes.

In adapting Shiu's proof to imaginary quadratic fields we encounter two difficulties. The first is the failure of unique factorization. Shiu's argument relies on the unique factorization of positive integers into positive primes, and we encounter obstructions from both the unit group (there is no analogue of ‘‘positive’’) and the class group. The obstruction from the unit group seems unavoidable, so we incorporated it into our results. We can handle the class group, however, and we prove an analogue of (2.1) for principal prime ideals. We introduce an *ad hoc* definition of congruences on ideals; namely, we write  $\mathfrak{p} \equiv a \pmod{q}$  if  $\mathfrak{p}$  is principal and any generator is congruent to  $a \pmod{q}$ . With this definition, we prove that there are sufficiently many prime ideals  $\equiv a \pmod{q}$  to make Shiu's argument work.

The second difficulty is geometric. Shiu's construction exhibits a string of primes, *almost* all of which are congruent to  $a \pmod{q}$ , after which finding a substring of primes  $\equiv a \pmod{q}$  is trivial. The two-dimensional analogue of this construction is no longer trivial: we find a

---

<sup>2</sup> We describe a simplified version of Shiu's argument which proves (1.1) for all  $a$ ; Shiu proves a better bound than (1.1) for certain moduli  $a \pmod{q}$ .

“bubble” in the complex plane containing many “good” primes  $\equiv ua \pmod{q}$  and few bad primes, and we want a smaller bubble containing only good primes. To obtain this, we count bad primes in larger bubbles than good primes, obtaining concentric bubbles in the complex plane. A combinatorial geometry argument (see Section 3) then allows us to find a bubble containing only good primes.

Generally speaking, the results of this paper indicate that the Maier matrix method “works” for imaginary quadratic fields (at least), and we believe that it should be possible to prove the existence of various irregularities in the distribution of the primes of  $\mathcal{O}_K$ , in analogy with results for  $\mathbb{Z}$  obtained by Maier [12], Granville and Soundararajan [8], and others. (We refer to the survey article of Granville [7] for an interesting overview of the method and additional related results.) This does present other difficulties however, and in any case we have not pursued this further here.

The outline of the paper is as follows. In Section 2 we prove several results related to the distribution of prime ideals in arithmetic progressions. The most important of these is a version of the prime number theorem for arithmetic progressions in quadratic fields (Theorem 2.4), and we closely follow Gallagher [6] for the proof. In Section 3 we present the combinatorial geometry argument which allows to find bubbles containing exclusively good primes. We conclude with the proof of Theorem 1.1 in Section 4.

**Setup and notation.** We assume  $K$  is an imaginary quadratic field with a fixed embedding  $K \rightarrow \mathbb{C}$ , with class number  $h_K$  and  $\#\mathcal{O}_K^\times = \omega = \omega_K \in \{2, 4, 6\}$ . Any  $K$ -dependence of implicit constants occurring in our results will be explicitly noted.

We will write  $\mathfrak{q} = (q)$  throughout, and where it does not lead to ambiguity we will refer to  $\mathfrak{q}$  and  $q$  interchangeably. We assume that the units of  $\mathcal{O}_K$  all represent distinct residue classes mod  $\mathfrak{q}$ ; by Lemma 2.2, this only excludes three choices for  $\mathfrak{q}$ . We further assume that the units do not represent all reduced residue classes modulo  $\mathfrak{q}$ ; if this happens then Theorem 1.1 is trivial.

As  $K$  will be fixed, we will simply write  $\phi(q)$  (or  $\phi(\mathfrak{q})$ ) for  $\phi_K(q) := |(\mathcal{O}_K/(q))^*|$ . We will also write  $h_{\mathfrak{q}}$  for  $h_K \phi(q)/\omega$ , the size of the ray class group.

Our methods oblige us to define congruences on ideals. For an ideal  $\mathfrak{b}$  of  $\mathcal{O}_K$  and  $a, q \in \mathcal{O}_K$ , we say that  $\mathfrak{b} \equiv a \pmod{q}$  if  $\mathfrak{b}$  is principal and  $b \equiv a \pmod{q}$  for any  $b$  for which  $\mathfrak{b} = (b)$ . If  $\mathfrak{b} \equiv a$ , then  $\mathfrak{b} \equiv ua$  for any unit  $u \in \mathcal{O}_K^\times$ . Equivalently, we see that  $\mathfrak{b} \equiv a \pmod{q}$  if  $\mathfrak{b}$  and  $(a)$  represent the same class in the ray class group  $H^{(q)}$ . For nonprincipal  $\mathfrak{b}$  we say that  $\mathfrak{b} \not\equiv a \pmod{q}$  for any  $a$ .

## ACKNOWLEDGEMENTS

I thank Bob Hough, Jorge Jiménez-Urroz, and an anonymous referee for useful advice and suggestions. In particular, I thank Hough for suggesting an improvement to a previous version of Proposition 3.1.

This work was part of my graduate thesis; I thank my advisor Ken Ono for his many useful suggestions, as well as the NSF for financial support.

## 2. PRIME IDEALS IN ARITHMETIC PROGRESSIONS

One standard ingredient in the Maier matrix method is a theorem of Gallagher ([6]; see also [11], Lemma 2), who proved that

$$(2.1) \quad \pi(x; q, a) = (1 + o_D(1)) \frac{x}{\phi(q) \log x},$$

uniformly in  $x \gg q^D$ , for a suitably large (infinite) set of moduli  $q$ . This result serves as a substitute for the Riemann hypothesis, and allows one to count the number of primes in Maier matrices in different arithmetic progressions.

The main goal of this section is generalize this result to imaginary quadratic fields. We will work with prime ideals rather than prime elements, to preserve unique factorization, and it will be necessary (if a bit unnatural) to describe the distribution of prime ideals in congruence classes.

**Definition 2.1.** *We write  $\pi_1(x; q, a)$  for the number of principal prime ideals  $\mathfrak{p}$  of norm  $\leq x$ , such that  $p \equiv a \pmod{q}$  for some generator  $p$  of  $\mathfrak{p}$ .*

We will estimate  $\pi_1(x; q, a)$  using analytic techniques applied to Hecke  $L$ -functions. We first recall the necessary definitions and terminology.

In place of  $\mathcal{O}_K/\mathfrak{q}$  we begin with the *ray class group* modulo  $\mathfrak{q}$

$$(2.2) \quad H^{\mathfrak{q}} := J^{\mathfrak{q}}/P^{\mathfrak{q}},$$

where  $J^{\mathfrak{q}}$  is the group of all fractional ideals coprime to  $\mathfrak{q}$ , and  $P^{\mathfrak{q}}$  is the group of principal fractional ideals  $(a) = (b)(c)^{-1}$  with  $b, c \in \mathcal{O}_K$  and  $b \equiv c \equiv 1 \pmod{\mathfrak{q}}$ . If we write  $J_1^{\mathfrak{q}}$  for the group of principal fractional ideals coprime to  $\mathfrak{q}$ , then  $J_1^{\mathfrak{q}}/P^{\mathfrak{q}}$  is in one-to-one correspondence with the set of sets of reduced residue classes modulo  $\mathfrak{q}$

$$(2.3) \quad \{ua : (a, \mathfrak{q}) = 1, u \in \mathcal{O}_K^{\times}\},$$

where  $a$  is a fixed in each set and  $u$  ranges over all units of  $\mathcal{O}_K$ . The proof of Theorem 1.1 will exhibit bubbles of prime elements  $p$ , such that the ideals  $(p)$  all lie in a fixed class in  $J_1^{\mathfrak{q}}/P^{\mathfrak{q}}$ .

Suppose henceforth that  $\mathfrak{q} \notin \{(2), (\frac{-3 \pm \sqrt{-3}}{2})\}$  and  $\phi(\mathfrak{q}) > 1$ . Then the size of the ray class group is given by the following simple formula.

**Lemma 2.2.** *If  $\mathfrak{q} \notin \{(2), (\frac{-3 \pm \sqrt{-3}}{2})\}$  and  $\phi(\mathfrak{q}) > 1$ , then we have*

$$(2.4) \quad h_{\mathfrak{q}} := |H^{\mathfrak{q}}| = h_K \phi(\mathfrak{q}) / \omega,$$

where  $h_K$  is the class number of  $K$ , and  $\omega \in \{2, 4, 6\}$  denotes the number of units of  $\mathcal{O}_K$ .

This is not difficult to show: as  $J^{\mathfrak{q}}/J_1^{\mathfrak{q}}$  is isomorphic to the usual class group, (2.4) follows by showing that there are  $\phi(\mathfrak{q})/\omega$  sets counted in (2.3), which in turn follows by showing that  $u - 1 \notin \mathfrak{q}$  for each unit  $u \neq 1$  of  $\mathcal{O}_K$ . This latter fact is easily checked (given the conditions on  $\mathfrak{q}$ ) and we omit the details.

*Remark.* In the case where  $\mathfrak{q} = \left(\frac{-3 \pm \sqrt{-3}}{2}\right)$  and  $K = \mathbb{Q}(\sqrt{-3})$ , the units of  $\mathcal{O}_K$  cover all reduced residue classes mod  $\mathfrak{q}$  and so the statement of Theorem 1.1 is empty.

From the group  $H^{\mathfrak{q}}$  we obtain *Hecke characters*  $\chi$  of  $K$  by lifting any character  $\chi$  of  $H^{\mathfrak{q}}$  to  $J^{\mathfrak{q}}$  in the obvious way, and setting  $\chi(\mathfrak{a}) = 0$  for any  $a$  not coprime to  $q$ . Throughout, we will only consider Hecke characters obtained in this fashion. (See, however, Chapter VII.6 of [13] (for example) for a more general discussion.) The associated *Hecke  $L$ -functions* are defined by the equation

$$(2.5) \quad L(s, \chi) := \sum_{\mathfrak{a}} \chi(\mathfrak{a})(\mathbb{N}\mathfrak{a})^{-s},$$

where  $\mathfrak{a}$  runs over all integral ideals of  $\mathcal{O}_K$ .

Our estimates for  $\pi_1(x; q, a)$  will depend on a zero-free region for the Hecke  $L$ -functions modulo  $\mathfrak{q}$ . For convenience, we formulate this hypothesis as *Hypothesis  $ZF(C)$* :

**Definition 2.3.** *If  $C > 0$ , we say that  $\mathfrak{q}$  satisfies Hypothesis  $ZF(C)$  if none of the Hecke  $L$ -functions modulo  $\mathfrak{q}$  have a zero in the region*

$$(2.6) \quad \sigma > 1 - C / \log[(\mathbb{N}q)(|t| + 1)].$$

*We say that  $q \in \mathcal{O}_K$  satisfies Hypothesis  $ZF(C)$  if the ideal  $(q)$  does.*

We will prove the following:

**Theorem 2.4.** *Suppose that  $q \in \mathcal{O}_K$  is not  $u$ ,  $2u$ , or  $\frac{-3 \pm \sqrt{-3}}{2}u$  for any unit  $u$  of  $\mathcal{O}_K$ , and that  $q$  satisfies Hypothesis  $ZF(C)$  for some  $C$ .*

*Then for  $D \geq 0$  we have*

$$\pi_1(2x; q, a) - \pi_1(x; q, a) = (\omega_K + o_{x,D}(1)) \frac{x}{h_K \phi_K(q) \log x},$$

*uniformly in  $q$  for  $(a, q) = 1$ ,  $\mathbb{N}q \geq |\Delta_K|$ , and  $x \geq \mathbb{N}q^D$ .*

Here  $o_{x,D}(1)$  denotes an error term bounded above by any  $\epsilon > 0$ , provided both  $x$  and  $D$  are chosen sufficiently large. The error term also depends on  $C$ , but in the application  $C$  will be an absolute constant.

We further remark that the condition  $\mathbb{N}q \geq |\Delta_K|$  is required only if the  $o_{x,D}(1)$  term is to be independent of  $K$ . Also, the restriction on  $q$  is not serious, as we may find primes in arithmetic progressions (mod  $q'$ ) for an appropriate multiple  $q'$  of  $q$ .

To use Theorem 2.4, we must prove that the zero-free region (2.6) holds for a suitably large (infinite) set of moduli. To define these moduli we introduce the notation

$$(2.7) \quad \mathcal{P}(y, q, \mathfrak{p}_0) := q \prod_{\mathbb{N}\mathfrak{p} \leq y; \mathfrak{p} \neq \mathfrak{p}_0} \mathfrak{p}.$$

**Proposition 2.5.** *For all sufficiently large  $x$  there exist an integer  $y$  and a prime  $\mathfrak{p}_0$  with  $x < \mathbb{N}\mathcal{P}(y, q, \mathfrak{p}_0) \ll x \log^3 x$  and  $\mathbb{N}\mathfrak{p}_0 \gg \log y$ , such that  $q$  satisfies Hypothesis  $ZF(C_2)$  for an absolute constant  $C_2$ .*

The proposition and its proof, given in Section 2.2, are the direct analogues of Theorem 1 of [15]. Note that the prime  $\mathfrak{p}_0$  is removed to ensure that the Siegel zero doesn't exist. The definition of “sufficiently large” depends on  $K$ . We could easily control the  $K$ -dependence here, but it would be more difficult in Lemma 2.9 and so we don't bother.

**2.1. Proof of Theorem 2.4.** Theorem 2.4 will follow from the following estimate:

**Proposition 2.6.** *If  $\mathfrak{q}$  satisfies Hypothesis  $ZF(C_1)$  and  $\max(\exp(\log^{1/2} x), \Delta_K) \leq \mathbb{N}\mathfrak{q} \leq x^b$  for a fixed constant  $b > 0$ , then we have*

$$(2.8) \quad \sum_{\chi} \left| \sum_{\mathbb{N}\mathfrak{p} \in [x, 2x]} \chi(\mathfrak{p}) \log(\mathbb{N}\mathfrak{p}) \right| \ll x \exp \left( -a \frac{\log x}{\log \mathbb{N}\mathfrak{q}} \right),$$

where the constant  $a$  depends only on  $C_1$ , the first sum is over all nonprincipal characters modulo  $\mathfrak{q}$ , and the implied constant is absolute.

With additional care, we expect to be able to prove a similar result for an arbitrary number field  $K$ .

Theorem 2.4 follows from Proposition 2.6 as follows: By the orthogonality relations, we have

$$\begin{aligned} \sum_{\substack{\mathbb{N}\mathfrak{p} \in [x, 2x] \\ \mathfrak{p} \equiv a \pmod{\mathfrak{q}}}} \log(\mathbb{N}\mathfrak{p}) &= \frac{1}{h_{\mathfrak{q}}} \sum_{\mathbb{N}\mathfrak{p} \in [x, 2x]} \sum_{\chi \pmod{\mathfrak{q}}} \bar{\chi}(a) \chi(\mathfrak{p}) \log(\mathbb{N}\mathfrak{p}) \\ &= \frac{1}{h_{\mathfrak{q}}} \sum_{\mathbb{N}\mathfrak{p} \in [x, 2x]} \log(\mathbb{N}\mathfrak{p}) + O \left( \frac{1}{h_{\mathfrak{q}}} \sum_{\chi \neq \chi_0} \left| \sum_{\mathbb{N}\mathfrak{p} \in [x, 2x]} \chi(\mathfrak{p}) \log(\mathbb{N}\mathfrak{p}) \right| \right), \end{aligned}$$

and for  $x \leq \exp((\log \mathbb{N}\mathfrak{q})^2)$ , the result now follows from the prime ideal theorem and Proposition 2.6.

For the (easier) range  $x > \exp((\log \mathbb{N}\mathfrak{q})^2)$ , a proof can be given as follows. Take  $T = \exp((\log x)^{3/4})$  in the proof of Proposition 2.6, and the quantity in (2.8) is  $\ll x \exp(-a(\log x)^{1/4})$ , which suffices for our result.

It therefore suffices to prove Proposition 2.6, and we will closely follow Gallagher [6]. Gallagher proves a similar result for Dirichlet  $L$ -functions, but with an additional sum over moduli  $q$ . He deduces his result from a log-free zero-density estimate for these  $L$ -functions, and in our case the appropriate zero-density estimate has been proved<sup>3</sup> by Fogels [5]:

**Proposition 2.7** (Fogels). *We have for any  $\mathfrak{q} \in \mathcal{O}_K$  and any  $T \geq \Delta_K \mathbb{N}\mathfrak{q}$*

$$(2.9) \quad \sum_{\chi} N_{\chi}(\alpha, T) \leq T^{c(1-\alpha)}.$$

Here  $N_{\chi}(\alpha, T)$  denotes the number of zeroes  $\rho = \beta + it$  of  $L(s, \chi)$  with  $\alpha < \beta < 1$  and  $|t| < T$ ,  $\chi$  ranges over all characters modulo  $\mathfrak{q}$ ,  $\Delta_K$  is the discriminant of  $K$ , and  $c$  is (for quadratic fields) an absolute constant.

<sup>3</sup> This is stated, in a slightly different form, after the main theorem of [5]. Note that Fogels published a corrigendum to [5], but that it does not affect the statement of the main results.

*Proof of Proposition 2.6.* At the outset, we choose  $T = (\mathbb{N}\mathbf{q})^2 \leq x^{1/2c}$ , which is an acceptable choice in all of our estimates.

By standard analytic techniques (see (5.53) and (5.65) of [9]), we have

$$(2.10) \quad \sum_{\mathbf{N}\mathbf{a} \in [x, 2x]} \chi(\mathbf{a}) \Lambda(\mathbf{a}) = \delta_\chi x - \sum_{\rho} \frac{(2x)^\rho - x^\rho}{\rho} + O\left(\frac{x \log^2 x}{T}\right),$$

where  $\delta_\chi$  is 1 or 0 according to whether  $\chi$  is principal or not,  $\Lambda(\mathbf{a}) := \log(\mathbb{N}\mathbf{p})$  if  $\mathbf{a}$  is a power of some prime  $\mathbf{p}$  and 0 otherwise, and  $\rho$  ranges over all the zeroes  $\rho = \beta + it$  of  $L(s, \chi)$  in the critical strip with  $|t| < T$ .

We observe that for each  $\rho = \beta + it$ ,

$$\frac{(2x)^\rho - x^\rho}{\rho} \ll x^\beta.$$

The terms where  $\mathbf{a}$  is a prime power (but not a prime) contribute  $\ll x^{1/2}$  to the sum (2.10) and so may be absorbed into the error term for  $T \leq x^{1/2}$ . Therefore, for nonprincipal  $\chi$  we see that

$$\sum_{\mathbf{N}\mathbf{p} \in [x, 2x]} \chi(\mathbf{p}) \log(\mathbb{N}\mathbf{p}) \ll \sum_{\rho} x^\beta + \frac{x \log^2 x}{T}.$$

Therefore,

$$\sum_{\chi \neq \chi_0} \left| \sum_{\mathbf{N}\mathbf{p} \in [x, 2x]} \chi(\mathbf{p}) \log(\mathbb{N}\mathbf{p}) \right| \ll \sum_{\chi \neq \chi_0} \sum_{\rho} x^\beta + \frac{x \log^2 x (\mathbb{N}\mathbf{q})}{T}.$$

The sum over  $\chi$  and  $\rho$  on the right is

$$(2.11) \quad - \int_0^1 x^\sigma d_\sigma \left( \sum_{\chi \neq \chi_0} N_\chi(\sigma, T) \right) = -x^\sigma \left( \sum_{\chi \neq \chi_0} N_\chi(\sigma, T) \right) \Big|_0^1 + \int_0^1 x^\sigma \log x \left( \sum_{\chi \neq \chi_0} N_\chi(\sigma, T) \right) d\sigma.$$

The first term of (2.11) is ([9], Theorem 5.8)

$$\sum_{\chi \neq \chi_0} N_\chi(0, T) \ll T \mathbb{N}\mathbf{q} \log(T \mathbb{N}\mathbf{q}).$$

Using the zero-free region (2.6) and Proposition 2.7, we see that the second term of (2.11) is

$$\ll \int_0^{1-C_1/\log[(\mathbb{N}\mathbf{q})(T+1)]} (x^\sigma \log x) T^{c(1-\sigma)} d\sigma.$$

Evaluating the integral above and recalling that  $T \leq x^{1/2c}$ , this second term is

$$\ll x \exp\left(-\frac{C_1}{2} \frac{\log x}{\log[(\mathbb{N}\mathbf{q})(T+1)]}\right).$$



We conclude from all these estimates that

$$\sum_{\chi}' \left| \sum_{\mathbb{N}\mathfrak{p} \in [x, 2x]} \chi(\mathfrak{p}) \log(\mathbb{N}\mathfrak{p}) \right| \ll \frac{(x \log^2 x) \mathbb{N}\mathfrak{q}}{T} + T \mathbb{N}\mathfrak{q} \log(T \mathbb{N}\mathfrak{q}) + x \exp\left(-\frac{C_1}{2} \frac{\log x}{\log[(\mathbb{N}\mathfrak{q})(T+1)]}\right).$$

With the choice  $T = (\mathbb{N}\mathfrak{q})^2$  and the hypothesis that  $\max(\exp(\log^{1/2} x), |\Delta_K|) \leq \mathbb{N}\mathfrak{q} \leq \min(x^{1/4c}, x^{1/4})$ , we obtain the proposition.  $\square$

**2.2. Proof of Proposition 2.5.** The proof follows Theorem 1 of [15]. We require the following zero-free region for Hecke  $L$ -functions, also due to Fogels [4]:

**Lemma 2.8** (Fogels). *Assume that  $\mathfrak{a}$  is an ideal of  $\mathcal{O}_K$  with  $|\Delta_K \mathbb{N}\mathfrak{a}|$  sufficiently large. Then  $\mathfrak{a}$  satisfies Hypothesis  $ZF(C_3)$  for an absolute constant  $C_3$ , with the possible exception of a single zero  $\beta$  of one Hecke  $L$ -function  $L(s, \chi)$  modulo  $\mathfrak{a}$ . If  $\beta$  exists then it must be real and satisfy*

$$(2.12) \quad \beta < 1 - (|\Delta_K| \mathbb{N}\mathfrak{a})^{-4}.$$

*Remark.* The above results in fact hold for an arbitrary number field  $K$ . In this case  $C$  depends on the degree of  $K$ , and the exponent  $-4$  in (2.12) should be replaced with  $-2[K : \mathbb{Q}]$ . As elsewhere in this paper, “sufficiently large” is allowed to depend on  $K$  (even for quadratic fields).

*Proof of Proposition 2.5.* Consider the product

$$(2.13) \quad \mathcal{P}'(y, q) := q \prod_{\mathbb{N}\mathfrak{p} \leq y} \mathfrak{p},$$

and suppose that an exceptional character mod  $\mathcal{P}'(y, q)$  exists; i.e., suppose that there exists a character  $\chi_1$  mod  $\mathcal{P}'(y, q)$  whose  $L$ -function has a real zero  $\beta$  in the range

$$(2.14) \quad 1 \geq \beta \geq 1 - \frac{C_3}{\log(|\Delta_K| \mathbb{N}\mathcal{P}'(y, q))}.$$

Write  $\chi'_1$  (mod  $\mathcal{P}''$ ) for the primitive character inducing  $\chi_1$ , so that  $\mathcal{P}'' | \mathcal{P}'(y, q)$ . Then comparing (2.14) with (2.12) we see<sup>4</sup> that  $\mathbb{N}\mathcal{P}'' \gg \frac{1}{|\Delta_K|} (\log \mathbb{N}\mathcal{P}'(y, q))^{1/4}$ . We thus see that for sufficiently large  $y$  (in terms of  $q$ ),  $\mathcal{P}''$  will have a prime divisor  $\mathfrak{p}_0$  satisfying  $\mathfrak{p}_0 \gg \log(\mathbb{N}\mathcal{P}'') \gg \log \log(\mathbb{N}\mathcal{P}'(y, q)) \gg \log y$ .

---

<sup>4</sup> If  $|\Delta_K|$  is small it might be the case that  $\mathcal{P}''$  is of too small norm to apply (2.12). For each such  $K$  we may choose a fixed ideal  $\mathfrak{b}$  of sufficiently large norm, and write  $\chi''_1$  for the character modulo  $\mathfrak{b}\mathcal{P}''$  induced by  $\chi'_1$ . The associated  $L$ -function will have a zero at the same spot, and we conclude that  $\mathbb{N}(\mathfrak{b}\mathcal{P}'') \gg \frac{1}{|\Delta_K|} (\log \mathbb{N}\mathcal{P}'(y, q))^{1/4}$ . As  $\mathfrak{b}$  is fixed for each  $K$ , this implies that  $\mathbb{N}\mathcal{P}'' \gg \frac{1}{|\Delta_K|} (\log \mathbb{N}\mathcal{P}'(y, q))^{1/4}$  as well.



We claim that there can be no character  $\chi_2$  modulo  $\mathcal{P}(y, q, \mathfrak{p}_0)$  whose  $L$ -function has a real zero in the region

$$(2.15) \quad \beta' > 1 - \frac{C_3}{2 \log(|\Delta_K| \mathbb{N}\mathcal{P}(y, q, \mathfrak{p}_0))}.$$

Assuming this for now, we see that  $\mathcal{P}(y, q, \mathfrak{p}_0)$  satisfies Hypothesis  $ZF(C_2)$  with  $C_2 := C_3/4$ , provided that  $y$  is large enough so that  $\mathbb{N}\mathcal{P}(y, q, \mathfrak{p}_0) \geq |\Delta_K|$ . To prove our claim, suppose such a  $\chi_2$  exists. Then  $\beta'$  will be in the region (2.14), and as  $\chi_2$  and  $\chi'_1$  induce different characters modulo  $\mathcal{P}'(y, q)$ ,  $\beta$  and  $\beta'$  will be zeroes to distinct  $L$ -functions modulo  $\mathcal{P}'(y, q)$  in the region (2.14), contradicting Lemma 2.8.

If no exceptional character mod  $\mathcal{P}'(y, q)$  exists, we choose  $\mathfrak{p}_0$  to be any prime divisor of  $\mathcal{P}'(y, q)$  of norm  $\geq \log y$ . We again take  $C_2 := C_3/4$  and see that (for large  $y$ ) no  $L$ -function modulo  $\mathcal{P}(y, q, \mathfrak{p}_0)$  will have a zero in the region (2.15).

To conclude, we must show that we can find a  $\mathcal{P}(y, q, \mathfrak{p}_0)$  in each range  $x < \mathbb{N}\mathcal{P}(y, q, \mathfrak{p}_0) \ll x \log^3 x$ . In quadratic fields there can exist at most two distinct primes of the same norm. For a fixed large  $y$ , let  $y' > y$  be minimal so that  $\mathcal{P}(y', q) \neq \mathcal{P}(y, q)$ . Then  $\mathbb{N}\mathcal{P}(y', q)/\mathbb{N}\mathcal{P}(y, q) \leq (y')^2 = (1 + o(1)) \log^2(\mathbb{N}\mathcal{P}(y', q))$ , so for any large  $x$  we can find  $y$  with  $2x \log x < \mathbb{N}\mathcal{P}(y, q) < 3x \log^3 x$ . Removing a prime  $\mathfrak{p}_0$  from our product we see that necessarily  $\mathbb{N}\mathfrak{p}_0 \leq y = (1 + o(1)) \log x$  and so  $x < \mathbb{N}\mathcal{P}(y, q, \mathfrak{p}_0) \ll x \log^3 x$ , as desired.  $\square$

**2.3. Additional lemmas.** We need two additional lemmas on the distribution of ideals with certain restrictions on their prime factors.

**Lemma 2.9.** *Let  $\mathcal{S}(x)$  denote the number of ideals of norm  $\leq x$  whose prime (ideal) factors are all  $\equiv 1 \pmod{\mathfrak{q}}$ . Then*

$$(2.16) \quad \mathcal{S}(x) = (C_{\mathfrak{q}} + o_{\mathfrak{q}}(1)) x (\log x)^{-1+1/h_{\mathfrak{q}}},$$

where

$$(2.17) \quad C_{\mathfrak{q}} := \frac{1}{\Gamma(1/h_{\mathfrak{q}})} \lim_{s \rightarrow 1^+} \left[ (s-1)^{1/h_{\mathfrak{q}}} \prod_{\mathfrak{p} \equiv 1 \pmod{\mathfrak{q}}} \left( 1 - \frac{1}{(\mathbb{N}\mathfrak{p})^{-s}} \right)^{-1} \right].$$

*Proof.* This is a generalization of Landau's work on sums of two squares, and also of Lemma 3 of [15]. Write

$$(2.18) \quad F(s) := \prod_{\mathfrak{p} \equiv 1 \pmod{\mathfrak{q}}} \left( 1 - \frac{1}{(\mathbb{N}\mathfrak{p})^{-s}} \right)^{-1}.$$

Then by a Tauberian theorem due to Raikov ([2], Theorem 2.4.1), the asymptotic (2.16) follows if we can write

$$F(s) = \frac{H(s)}{(s-1)^{1/h_{\mathfrak{q}}}}$$

for a function  $H(s)$  which is holomorphic and nonzero in the region  $\Re(s) \geq 1$ , with

$$C_{\mathfrak{q}} = \frac{H(1)}{\Gamma(1/h_{\mathfrak{q}})}.$$

We write

$$(2.19) \quad \Theta(s) := \frac{\prod_{\chi \pmod{\mathfrak{q}}} L(s, \chi)}{F(s)^{h_{\mathfrak{q}}}},$$

and computing the Dirichlet series expansion for  $\log \Theta(s)$  (exactly as in [15]) we conclude that  $\Theta(s)$  is holomorphic for  $\Re(s) > \frac{1}{2}$ . The product  $\prod_{\chi \pmod{\mathfrak{q}}} L(s, \chi)$  has a simple pole at  $s = 1$ , and is otherwise holomorphic and nonzero in  $\Re(s) \geq 1$ . The result follows.  $\square$

We now need a result from the theory of ‘smooth’ numbers, i.e., numbers whose prime factors are all sufficiently small. (See, for example, Chapter III.5 of Tenenbaum’s book [16] for a general introduction to the theory.) Here we require a result for ‘smooth’ algebraic integers in  $K$ .

**Lemma 2.10.** *Let  $\Psi_K(x, y)$  be the number of ideals of norm  $< x$  which are composed only of primes with norm  $< y$ , and write  $u := \log x / \log y$ . Then for  $1 \leq u \leq \exp(c(\log y)^{3/5-\epsilon})$  (for a certain constant  $c$ ) we have*

$$(2.20) \quad \Psi_K(x, y) \ll_K x \log^2 y \exp(-u(\log u + \log \log u + O(1))).$$

*Proof.* This follows immediately by comparing results of de Bruijn [1] and Krause [10]. de Bruijn proved (2.20) for  $K = \mathbb{Q}$ . For general  $K$ , Krause proved an asymptotic formula for  $\Psi_K(x, y)$  in terms of the Dickman function, and Krause’s result implies in particular that for  $u$  in the range specified,

$$\lim_{x, y \rightarrow \infty} \frac{\Psi_K(x, y)}{\Psi(x, y)} = \text{res}_{s=1} \zeta_K(s),$$

where  $\zeta_K(s)$  denotes the Dedekind zeta function. The lemma then follows immediately.  $\square$

### 3. BUBBLES OF GOOD AND BAD POINTS

Suppose we are given a set of integers,  $g$  of which are “good” and  $b$  of which are “bad”. Trivially, this set contains a string of  $\gg g/b$  consecutive good integers. In this section we prove a two-dimensional analogue of this statement.

We formulate our result as a general proposition in combinatorial geometry. Suppose some circle in the plane contains (in its interior)  $g$  “good” points and  $b$  “bad” points. (In our application, these will be prime elements of  $\mathcal{O}_K$  congruent and not congruent to  $ua \pmod{q}$ , respectively.) We would like to find a smaller circle containing  $\gg g/b$  good points and no bad ones. We must find this entirely within the original circle, as there may be additional bad points outside this circle which we have not counted.

This is too much to ask for in general; for example, we cannot find such a smaller circle if the good points are all close to the boundary and the bad points are spread evenly. To avoid such counterexamples, we count good and bad points in concentric circles as follows:

**Proposition 3.1.** *Suppose the plane contains some number of “good” and “bad” points, that the unit circle contains  $g$  good points, and that the circle  $|z| < 3$  contains  $b$  bad points. Then there exists some circle in the plane containing  $> g/(2b + 12)$  good points and no bad points.*

*Remark.* In our application to the proof of Theorem 1.1,  $b$  and  $g$  will be large with  $b = o(g)$ . The construction will be scaled and translated to appropriate regions of the complex plane.

For the proof we require the following geometric construction:

**Lemma 3.2.** *Let  $\mathcal{P}$  be a set of points  $N$  in the plane, not all collinear. Then there exists a triangulation (called a Delaunay triangulation) of  $\mathcal{P}$ , such that no point of  $\mathcal{P}$  is inside the circumcircle of any triangle. This triangulation consists of  $2N - 2 - k$  triangles, where  $k$  is the number of points in  $\mathcal{P}$  lying on the boundary of the convex hull of  $\mathcal{P}$ .*

See, e.g., Chapter 9 of [3] for a proof of this. Observe also that if all points of  $\mathcal{P}$  are collinear, then Proposition 3.1 is trivial.

*Proof of Proposition 3.1.* The proof is by geometric construction. Write  $V$  for the set of all bad points of distance less than 3 from the origin, together with the 7-gon consisting of the points  $2e^{2\pi i n/7}$ , for  $n \in \mathbb{Z}$ .

Construct the Delaunay triangulation  $T$  of  $V$ , let  $\mathcal{C}$  be the set of circumcircles of all triangles in  $T$ , and let  $\mathcal{C}' \subseteq \mathcal{C}$  be those circles which nontrivially intersect the interior of the unit circle. By construction, no circle in  $\mathcal{C}'$  contains any point of  $V$ , and the circles in  $\mathcal{C}'$  cover the interior of  $C(1)$ , with the exception of any bad points.

We claim that every circle in  $\mathcal{C}'$  is contained inside  $\{|z| = 3\}$ . Supposing this for now, we know that the circles in  $\mathcal{C}'$  do not contain any bad points, including any which lie on or outside  $\{|z| = 3\}$ . These circles do contain all of the good points in the unit circle, and it follows that one such circle contains  $\geq g/|\mathcal{C}'|$  good points. Lemma 3.2 implies that  $|\mathcal{C}'| < 2(b + 7) - 2$  as required.

To prove that every circle in  $\mathcal{C}'$  is contained inside  $\{|z| = 3\}$ , suppose that  $C$  is a counterexample. Then  $C$  or its interior will contain points  $P_1$  and  $P_3$  with  $|P_1| = 1$  and  $|P_3| = 3$ . Furthermore, we may take these points to be on the ray from the origin going through the center of  $C$ . We also easily check that  $C$  must contain the circle having  $\overline{P_1 P_3}$  as its diameter.

For some point  $Q$  of the 7-gon, the angle between  $\overrightarrow{OQ}$  and  $\overrightarrow{OP_3}$  is at most  $\pi/7$  and in particular is less than  $\pi/6$ . We check that the distance between  $Q$  and the midpoint of  $\overline{P_1 P_3}$  is then less than 1, which implies that  $Q$  is contained in the interior of  $C$ , our contradiction.  $\square$

*Remark.* We thank Bob Hough, who suggested an improvement which improved the statement of Proposition 3.1 and simplified its proof.

## 4. PROOF OF THEOREM 1.1

We fix  $K$ ,  $\mathfrak{q} = (q)$ , and  $a$ ; we assume that the units of  $\mathcal{O}_K$  do not represent all the reduced residue classes modulo  $\mathfrak{q}$ , and that the residue classes represented are all distinct. Except where noted, implied constants in our analysis do not depend on  $\mathfrak{q}$ . We assume a sufficiently large (in terms of  $\mathfrak{q}$  and  $K$ ) integer  $x$  is given, and choose  $D > 3$  such that the term  $o_{x,D}(1)$  of Theorem 2.4 is bounded by  $\frac{1}{2}$ .

Our proof consists of three steps. In the first step, we find a modulus  $Q$  such that any  $b \in \mathcal{O}_K$  of small norm which is coprime to  $Q$  is very likely to be congruent to  $ua \pmod{Q}$ . In the second step, we use this  $Q$  to construct a Maier matrix of elements of  $\mathcal{O}_K$ , such that nearly all of the primes in the matrix are  $\equiv ua \pmod{Q}$ . In the final step, we argue that this Maier matrix contains a bubble of congruent primes, and bound its size from below.

**The modulus  $Q$ .** We use Proposition 2.5 to choose  $y$  and  $\mathfrak{p}_0$  such that

$$x^{1/D} < \mathcal{NP}(y, q, \mathfrak{p}_0) \ll x^{1/D} \log x$$

and such that  $\mathcal{P}(y, q, \mathfrak{p}_0)$  satisfies Hypothesis  $ZF(C_2)$ . We introduce variables  $z < y$  and  $t < (yz)^{1/2}$  with  $z = o(t)$ , and define a set of primes  $\mathcal{P}$  as follows: If  $a$  is not congruent to a unit modulo  $\mathfrak{q}$ , we define

$$(4.1) \quad \mathcal{P} := \begin{cases} \{\mathfrak{p} : \mathbb{N}\mathfrak{p} \leq y, \mathfrak{p} \neq \mathfrak{p}_0, \mathfrak{p} \not\equiv 1, a \pmod{\mathfrak{q}}\} \\ \cup \{\mathfrak{p} : t \leq \mathbb{N}\mathfrak{p} \leq y, \mathfrak{p} \neq \mathfrak{p}_0, \mathfrak{p} \equiv 1 \pmod{\mathfrak{q}}\} \\ \cup \{\mathfrak{p} : \mathbb{N}\mathfrak{p} \leq yz/t, \mathfrak{p} \neq \mathfrak{p}_0, \mathfrak{p} \equiv a \pmod{\mathfrak{q}}\}. \end{cases}$$

If  $a$  is congruent to a unit modulo  $\mathfrak{q}$ , we define instead

$$(4.2) \quad \mathcal{P} := \begin{cases} \{\mathfrak{p} : \mathbb{N}\mathfrak{p} \leq y, \mathfrak{p} \neq \mathfrak{p}_0, \mathfrak{p} \not\equiv 1 \pmod{\mathfrak{q}}\} \\ \cup \{\mathfrak{p} : t \leq \mathbb{N}\mathfrak{p} \leq yz/t, \mathfrak{p} \neq \mathfrak{p}_0, \mathfrak{p} \equiv 1 \pmod{\mathfrak{q}}\}. \end{cases}$$

We recall our convention that a nonprincipal prime ideal  $\mathfrak{p}$  is not  $\equiv a \pmod{\mathfrak{q}}$  for any  $\mathfrak{q}$ .

The latter definition (4.2) is motivated by simplicity, as it allows us to treat both cases simultaneously. Following Shiu [15], it should be possible to define  $\mathcal{P}$  differently in this case, and modestly improve our result for a certain subset of moduli  $a$ .

We further define

$$(4.3) \quad \mathfrak{Q} = (Q) := \mathfrak{q} \prod_{\substack{\mathfrak{p} \in \mathcal{P} \\ \mathfrak{p} \neq \mathfrak{p}_1}} \mathfrak{p},$$

where  $\mathfrak{p}_1$  is any prime ideal with  $\log y < \mathbb{N}\mathfrak{p}_1 \leq y$  for which  $\mathfrak{Q}$  is principal. We may then write  $Q$  for any generator of  $\mathfrak{Q}$ .

We see that  $\mathfrak{Q}|\mathcal{P}(y, q, \mathfrak{p}_0)$  and  $\log(\mathbb{N}Q) \geq \frac{1}{3} \log(\mathcal{NP}(y, q, \mathfrak{p}_0))$ . Proposition 2.5 thus implies that the Hecke  $L$ -functions modulo  $\mathfrak{Q}$  have no zeroes in the region

$$(4.4) \quad 1 \geq \Re s > 1 - \frac{C_2}{3 \log[(\mathbb{N}Q)(|t| + 1)]},$$

as any such zeroes would induce zeroes of  $L$ -functions modulo  $\mathcal{P}(y, q, \mathfrak{p}_0)$  at the same point, contrary to Hypothesis  $ZF(C_2)$  for  $\mathcal{P}(y, q, \mathfrak{p}_0)$ . In other words  $Q$  satisfies Hypothesis  $ZF(C)$  with  $C := C_2/3$ , so that the primes are well-distributed (i.e., Theorem 2.4 holds) in arithmetic progressions modulo  $Q$ .

**Construction of the Maier matrix.** Our construction adapts that of Shiu. In our case, the geometrical argument given in Section 3 requires us to keep track of more “bad” primes than “good”. Thus we define “bubbles”  $B$  and  $B'$  consisting of those elements of  $\mathcal{O}_K$  whose norm is less than  $yz$  and  $9yz$ , respectively. We further define Maier matrices  $M$  and  $M'$ , with  $(i, b)$  entry equal to the algebraic integer  $iQ + b$ , where  $i$  ranges over all elements of  $\mathcal{O}_K$  with norm in  $(\mathbb{N}Q^{D-1}, 2\mathbb{N}Q^{D-1})$ , and  $b$  ranges over elements of  $B$  and  $B'$  respectively. We regard  $M$  naturally as a submatrix of  $M'$ .

We define sets

$$(4.5) \quad S := \{b \in B; (b, Q) = 1; b \equiv ua \pmod{q} \text{ for some } u \in \mathcal{O}_K^\times\}$$

and

$$(4.6) \quad T := \{b \in B'; (b, Q) = 1; b \not\equiv ua \pmod{q} \text{ for any } u \in \mathcal{O}_K^\times\}.$$

We will prove that  $S$  is much larger than  $T$ .

To estimate  $S$ , we observe that most elements of  $S$  are uniquely determined as elements of the form  $pn$ , where  $p$  is a prime of norm  $> yz/t$  and is congruent to  $ua$  for some unit  $u$ , and  $n$  is a product of primes congruent to 1 modulo  $q$ . (There will also be multiples of  $\mathfrak{p}_0$  and  $\mathfrak{p}_1$ , which we ignore.) Subdividing dyadically, we see that

$$\begin{aligned} |S| &\geq \sum_{i=0}^{\lfloor \frac{\log t}{\log 2} \rfloor - 2} \left( \pi_1(2^{i+1}yz/t; q, ua) - \pi_1(2^i yz/t; q, ua) \right) \mathcal{S}(t/2^{i+1}) \\ &\gg \frac{C_q}{h_q} \sum_{i=0}^{\lfloor \frac{\log t}{\log 2} \rfloor - i_0} \left( \frac{yz2^i}{t \log y} \right) \cdot \frac{t}{2^{i+1}} \log(t/2^{i+1})^{-1+1/h_q}. \end{aligned}$$

Here  $i_0$  is a constant, depending on  $q$ , such that Lemma 2.9 gives an asymptotic estimate for  $x \gg 2^{i_0}$ . We now simplify and approximate the sum by the corresponding integral, and conclude that

$$\begin{aligned} (4.7) \quad |S| &\gg \frac{C_q yz}{h_q \log y} \int_0^{\frac{\log t}{\log 2} - i_0} (\log t - s \log 2)^{-1+1/h_q} ds \\ &= \frac{C_q yz}{(\log 2)(\log y)} \left( (\log t)^{1/h_q} - (i_0 \log 2)^{1/h_q} \right) \gg \frac{C_q yz}{\log y} (\log t)^{1/h_q}. \end{aligned}$$

Elements of  $T$  come in three types: multiples of  $\mathfrak{p}_0$  and  $\mathfrak{p}_1$ , multiples of a prime of norm greater than  $y$ , or products of a unit and elements whose norms are less than  $t$  and are congruent to 1 modulo  $q$ . We write  $T', T'', T'''$  for these subsets of  $T$  respectively and we will

estimate each in turn. We have  $|T'| \ll yz / \log y$  because  $\mathbb{N}\mathfrak{p}_0, \mathbb{N}\mathfrak{p}_1 \gg \log y$ . For  $T''$ , we have that

$$\begin{aligned} |T''| &\leq \sum_{i=0}^{\lceil \frac{\log(9z)}{\log 2} \rceil - i_0} \left( \pi_1(2^{i+1}y) - \pi_1(2^i y) \right) \mathcal{S}(9z/2^i) + \left( \pi_1(9yz) - \pi_1(yz/2^{i_0}) \right) \mathcal{S}(9 \cdot 2^{i_0}). \\ &\ll \sum_{i=0}^{\lceil \frac{\log(9z)}{\log 2} \rceil - i_0} \left( \frac{2^i \omega y}{h_K \log y} \right) \cdot \frac{C_q z}{2^i} (\log(9z/2^i))^{-1+1/h_q} + O_q \left( \frac{yz}{\log y} \right). \end{aligned}$$

In the above,  $\pi_1(x)$  counts the number of principal prime ideals of norm  $\leq x$ . Estimating in the same way as in (4.7), we conclude that

$$|T''| \ll C_q \phi(q) \frac{yz(\log z)^{1/h_q}}{\log y}.$$

To count elements  $T'''$  we apply Lemma 2.10. We choose (as in [15])

$$(4.8) \quad t = \exp \left( \frac{\log y \log \log \log y}{4 \log \log y} \right),$$

and the lemma implies that

$$|T'''| = \omega \Psi(yz, t) \ll yz(\log t)^2 \exp(-4 \log \log y + o(\log \log y)) \ll \frac{yz}{\log y}.$$

Putting these estimates together we conclude that

$$(4.9) \quad |T| \ll C_q \phi(q) \frac{yz(\log z)^{1/h_q}}{\log y}.$$

If  $y$  is large in terms of  $K$ , then the implied constant does not depend on  $K$ .

Write  $P_1$  for the number of primes in  $M$  (henceforth “good primes”) congruent to  $ua$  modulo  $q$  for any unit  $u \in \mathcal{O}_K$ , and write  $P_2$  for the number of primes (“bad primes”) in  $M'$  not congruent to  $ua$  for any  $u$ . By Theorem 2.4,  $P_1$  and  $P_2$  are determined by  $|S|$  and  $|T|$ , up to an error term which can be made small by choosing large  $x$  and  $D$ . We therefore conclude that

$$(4.10) \quad P_1 \gg C_q \frac{yz(\log t)^{1/h_q}}{\log y} \frac{\mathbb{N}Q^D}{\phi(Q) \log(\mathbb{N}Q^D)}$$

and

$$P_2 \ll C_q \phi(q) \frac{yz(\log z)^{1/h_q}}{\log y} \frac{\mathbb{N}Q^D}{\phi(Q) \log(\mathbb{N}Q^D)}.$$

**Finding a bubble of congruent primes.** We will split into two cases and compare numbers of good and bad primes. Throughout, we count all bad primes appearing in  $M'$  (which contains  $M$ ), but only those good primes appearing in  $M$ .

In the first case the majority of good primes occur in rows containing at least one bad prime, in which case the proportion of good to bad primes in some such row of  $M'$  is  $\gg |S|/|T|$ . These primes all occur in some circle in  $\mathbb{C}$  of radius  $3\sqrt{yz}$ , and applying Proposition 3.1 we see that this circle contains a subcircle with  $\gg |S|/|T|$  good primes and no bad primes, which is our desired bubble of congruent primes. The number of primes in the bubble will be

$$\gg |S|/|T| \gg \frac{1}{\phi(q)} \left( \frac{\log t}{\log z} \right)^{1/h_q}.$$

In the second case, the majority of good primes occur in rows not containing any bad primes. These such rows then constitute bubbles of congruent primes of radius  $3\sqrt{yz}$ , and at least one will contain  $\gg P_1/R$  primes, where  $R$  denotes the number of rows, i.e., the number of elements of  $\mathcal{O}_K$  with norm in  $(\mathbb{N}Q^{D-1}, 2\mathbb{N}Q^{D-1})$ . As  $\mathcal{O}_K$  forms a lattice in  $\mathbb{C}$  we have  $R \sim C_K \mathbb{N}Q^{D-1}$  for some constant  $C_K$  depending on  $K$ . Using (4.10), we see that some row of  $M$  will be a bubble containing

$$\gg_K C_q \frac{yz(\log t)^{1/h_q}}{\log y} \frac{\mathbb{N}Q}{\phi(Q) \log(\mathbb{N}Q^D)}$$

primes. Now we have

$$\log(\mathbb{N}Q) \ll \sum_{\mathbb{N}\mathfrak{p} \leq y} \log(\mathbb{N}\mathfrak{p}) \ll y,$$

and

$$(4.11) \quad \frac{\mathbb{N}Q}{\phi(Q)} = \frac{\mathbb{N}\mathfrak{q}}{\phi(\mathfrak{q})} \prod_{\mathfrak{p} \in \mathcal{P}} \left( 1 - \frac{1}{\mathbb{N}\mathfrak{p}} \right)^{-1} \gg_{\mathfrak{q}} \log y (\log t)^{-1/h_q}.$$

To prove (4.11), one can use a result of Rosen (Theorem 4 of [14], along with the result of Landau cited immediately afterwards). The result is then easily proved, provided that the dependence on  $\mathfrak{q}$  (and  $K$ ) is allowed.

Combining these results, we conclude that this bubble contains  $\gg_{\mathfrak{q}} z$  primes. Therefore, our argument produces a bubble of

$$\gg \min \left( \frac{1}{\phi(q)} \left( \frac{\log t}{\log z} \right)^{1/h_q}, C'_q z \right)$$

congruent primes, for a constant  $C'_q$  depending on  $\mathfrak{q}$ . Our theorem follows by choosing  $z = \log \log(\mathbb{N}Q)$ .

## REFERENCES

- [1] N. G. de Bruijn, *On the number of positive integers  $\leq x$  and free of prime factors  $\geq y$* , Indag. Math. **13** (1951), 50-60.
- [2] A. C. Cojocaru and M. R. Murty, *An introduction to sieve methods and their applications*, Cambridge University Press, Cambridge, 2005.
- [3] M. de Berg, M. van Kreveld, M. Overmars, and O. Schwarzkopf, *Computational geometry: algorithms and applications*, Springer-Verlag, Berlin, 2000.
- [4] E. Fogels, *On the zeros of Hecke's L-functions I*, Acta Arith. **7** (1961), 131-147.



- [5] E. Fogels, *On the zeros of  $L$ -functions*, Acta Arith. **11** (1965), 67-96; corrigendum, Acta Arith. **14** (1967/1968), 435.
- [6] P. X. Gallagher, *A large sieve density estimate near  $\sigma = 1$* , Invent. Math. **11** (1970), 329-339.
- [7] A. Granville, *Unexpected irregularities in the distribution of prime numbers*, Proceedings of the International Congress of Mathematicians (Zürich, 1994), 388-399, Birkhäuser, Basel, 1995.
- [8] A. Granville and K. Soundararajan, *An uncertainty principle for arithmetic sequences*, Ann. of Math. **165** (2007), no. 2, 593-635.
- [9] H. Iwaniec and E. Kowalski, *Analytic number theory*, American Mathematical Society, Providence, 2005.
- [10] U. Krause, *Abschätzungen für die Funktion  $\Psi_K(x, y)$  in algebraischen Zahlkörpern*, Manuscripta Math. **69** (1990), 319-331.
- [11] H. Maier, *Chains of large gaps between consecutive primes*, Adv. in Math. **39** (1981), 257-269.
- [12] H. Maier, *Primes in short intervals*, Michigan Math. J. **32** (1985), 221-225.
- [13] J. Neukirch, *Algebraic number theory*, Springer-Verlag, Berlin, 1999.
- [14] M. Rosen, *A generalization of Mertens' theorem*, J. Ramanujan Math. Soc. **14** (1999), 1-19.
- [15] D. K. L. Shiu, *Strings of congruent primes*, J. London Math. Soc. **61** (2000), 359-373.
- [16] G. Tenenbaum, *Introduction to analytic and probabilistic number theory*, Cambridge University Press, Cambridge, 1995.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF SOUTH CAROLINA, 1523 GREENE STREET, COLUMBIA, SC 29208

*E-mail address:* thorne@math.sc.edu